PATENT APPLICATION

NETWORK COPY PROTECTION FOR DATABASE PROGRAMS

Inventors: 1. Jonathan Thatcher
343 Paul Avenue
Mountain View, CA 94041
US Citizen

2. Clay Maeckel
1498 Via Contenta
San Jose, CA 95128
US Citizen

Assignee: Apple Computer, Inc.

BEYER WEAVER & THOMAS, LLP
P.O. Box 778
Berkeley, CA 94704-0778
(650) 961-8300

NETWORK COPY PROTECTION FOR DATABASE PROGRAMS

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to databases and, more particularly, to Network Copy Protection (NCP) of database programs.

2. Description of the Related Art

Databases are used to store data in a manner that facilitates subsequent use of the data. A database includes one or more files, each of which contain one or more records. A record holds information about a subject or item in its various fields.

To allow a user to more easily access and manage data stored in databases, database programs have recently been developed. Database programs, among other things, often provide a user interface which allows the user to conveniently interact with the database program. By interacting with the user interface, the user of the database can perform various operations on the data stored in the database. The interface provided by the database program is typically a Graphical User Interface which allows the user to conveniently interact with the database program and, in turn, with the database. The user may interact with the graphical user interface to, for example, view the data in various

ways. The visual representations provided to the user can include, for example, a browse mode. The browse mode allows records to be viewed, changed, sorted, deleted, or added.

Fig. 1 is a representative screen depiction from a conventional database program, namely, FileMaker Pro 4.0 by FileMaker Pro, Inc. of Santa Clara, California. The screen depiction pertains to an asset management database having three records. A browse mode for the first record of the ASSET MANAGEMENT database is depicted. The browse mode is suitable for on-line or screen viewing of the records of the asset management database and allows the records to be viewed or deleted. The data in the fields of the record can be changed, sorted, deleted or added in the browse mode.

Accordingly, the database program provides the user with the ability to conveniently access data which is stored locally in the database. It should be noted that the database program may also provide the capability to access data that is stored in a remote location. For example, the database program can be connected to another database program over a computer network. In this situation, one database program can act as a "guest" and establish a connection to the other database program ("host" database program). Via its connection to the host database program, the guest database program can, in turn, provide the user with access to data stored remotely.

One important goal is providing Network Copy Protection (NCP) for database programs. This means that only licensed copies of database programs should be allowed to operate (e.g., connect to another database program and access data remotely). In other words, if only one software license has been issued for a database program, two copies of the same data program should not be able to connect to another database program to access data.

Typically, a unique installation code is assigned to each licensed copy of database programs. The user is required to enter the installation code when the database program is installed. After the database program has been correctly installed with the installation code, every time the database program is started (or

connects to the computer network) a check can be made to verify the installation code is not already in use. Conventionally, the database program does not make this verification itself. Rather, a naming (or name binding) protocol is utilized to make the verification depending on platform and/or connection protocol used by

5   the database program. For example, the AppleTalk name binding protocol is used in Macintosh environments and the Network Basic Input Output System (NetBios) naming protocol is used in Windows environments. Thus, to implement Network Copy Protection for database programs, conventionally, a specific naming protocol is used depending on the particular platform and/or the

10   connection protocol that is used.

One problem with using specific name binding protocols to handle Network Copy Protection is that this approach fails to detect copies of the same database when different platforms and/or different connection protocols are used. For example, if one copy of the database program is operating in the

15   Windows environment and another copy of the same database program is operating in the Macintosh environment, the conventional approach fails to detect that two instances of the same database program are operating. Similarly, this failure can occur when two copies of the same database program are using different communication protocols.

20   Another problem is that the name binding protocols used by the conventional data programs are becoming obsolete, as more widely accepted connection protocols are becoming more prevalent. One prevalent protocol that has gained wide acceptance is Transmission Control Protocol (TCP). As such, both the Windows and the Macintosh environments support TCP.

25   Unfortunately, however, TCP does not provide a suitable naming protocol that can readily be used to implement Network Copy Protection for database programs. Moreover, it is highly desirable to provide Network Copy Protection that can function across various platforms and connection protocols.

In view of the foregoing, there is a need for improved Network Copy

30   Protection for database programs.

SUMMARY OF THE INVENTION

Broadly speaking, the invention relates to Network Copy Protection for database programs. In accordance with one embodiment of the invention, a database program capable of providing Network Copy Protection across various platforms and/or connection protocols is disclosed. Accordingly, the database program can detect unlicensed use of the software even when different platforms and/or connection protocols are used by two instances (software copies) of the same database program. When unlicensed use of software is detected, access to data will be denied by the database program. As will be appreciated, in addition to supporting more conventional communication protocols, the database program can support more prevalent connection protocols (e.g., TCP).

The invention can be implemented in numerous ways, including as a method, an apparatus, a computer readable medium, and a database system. Several embodiments of the invention are discussed below.

As a method for providing network copy protection for database programs operating in a computer network, one embodiment of the invention includes the acts of: sending a request for connection, said request being sent by a first database program to a second database program operating on the computer network; determining whether another copy of the first database program is connected to the second database program; and granting the request for connection to the first database program when it is determined that another copy of the guest database program is not connected to the database program.

As a database program operating on a computer network, one embodiment of the invention includes a first database program suitable for accessing data stored in a database. The first database program is capable of providing access to a second database program connected to the computer network. The access is provided to allow the second database program to access data stored in the database associated with the first database program. The first database program is capable of detecting whether the second database is a

software copy of another database program, even if the second database program and its copy are operating in different platforms.

As another method for providing network copy protection for database programs operating in a computer network, another embodiment of the invention includes the acts of: sending an installation code identifier with session information to a host database program, the session information being sent by a guest database program to the host database program; determining whether the code identifier is in a list of connected guests, the list of connected guests including one or more installation code identifiers which are respectively associated with one or more guest database programs that are connected to the host database program; and establishing a connection between the guest and host database programs when it is determined that that the code identifier is not in a list of connected guests; and not establishing a connection between the guest and host database programs when it is determined that said code identifier is in a list of connected guests.

As a computer readable media including computer program code for providing network copy protection for database programs operating in a computer network, one embodiment of the invention includes: computer program code for sending a request for connection, the request being sent by a first database program to a second database program operating on the computer network; computer program code for determining whether another copy of the first database program is connected to the second database program; and computer program code for granting the request for connection to the first database program only when it is determined that another copy of the guest database program is not connected to the database program.

The advantages of the invention are numerous. Different embodiments or implementations may yield one or more of the following advantages. One advantage of the invention is that Network Copy Protection can be implemented for database programs operating on various software platforms. Another advantage of the invention is that that copy protection can be effectively provided even if different connection protocols are used by the database programs. Still another advantage is

that the invention can be implemented to operate in an efficient manner and without significant change to the existing connection protocols and/or database programs. Yet another advantage of the invention is that Network Copy Protection can be implemented for more prevalent connection protocols.

5   Other aspects and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating by way of example the principles of the invention.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

Fig. 1 is a representative screen depiction from a conventional database program.

Fig. 2A illustrates a computer network in accordance with one embodiment of the invention.

Fig. 2B depicts a computer network in accordance with another embodiment of the invention.

Fig. 3 illustrates a method for providing Network Copy Protection in accordance with one embodiment of the invention.

Fig. 4 illustrates in greater detail a method for providing Network Copy Protection in accordance with another embodiment of the invention.

Fig. 5 is a block diagram representation of session information transmitted in accordance with one embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

As noted in the background of the invention, there is a need for improved Network Copy Protection for database programs. More particularly, there is a need for database programs that, among other things, provide Network Copy Protection across various platforms and/or connection protocols.

Accordingly, the invention pertains to improved Network Copy Protection for database programs. In accordance with one embodiment of the invention, a database program capable of providing Network Copy Protection across various platforms and/or connection protocols is disclosed. Accordingly, the database program can detect unlicensed use of the software even when different platforms and/or connection protocols are used by two instances (software copies) of the same database program. When unlicensed use of software is detected, access to data will be denied by the database program. As will be appreciated, in addition to supporting more conventional communication protocols, the database program can support more prevalent connection protocols (e.g., TCP).

Embodiments of these aspects of the invention are discussed below with reference to Figs. 2A - 5. However, those skilled in the art will readily appreciate that the detailed description given herein with respect to these figures is for explanatory purposes as the invention extends beyond these limited embodiments.

Fig. 2A illustrates a computer network 200 in accordance with one embodiment of the invention. As shown in Fig. 2A, a database program 202 is connected to the computer network 200. The database program 202 can provide access to data stored on a database 204. The database 204 is typically stored at a site local to the database program 202. In addition to providing access to the database 204, the database program 202 may provide access to data stored in a database 206. It should be noted that the database 206 can be at a remote location with respect to the database 204 and database program 202. To access the remote database 206, the database program 202 establishes a

connection to a database program 208. The database program 208 is also connected to the computer network 200. Accordingly, the database program 202 can establish a connection with the database 206 over the computer network 200 via a communication medium 210. When database program 202 is accessing the database 206 through the database program 208, the database program 202 can be referred to as the "guest" database program. In this situation, the database program 208 can be referred to as the "host" database program.

As will be appreciated, the database programs 202 and 208 can be in a "peer to peer" relationship with each other. In other words, both of the data base programs 202 and 208 can act as a guest or a host with respect to each other. This means that the database program 208 may also act as a "guest" and access the database 204 through the database program 202.

In any case, the guest database program typically sends a request for connection to the host database program over the computer network 200. The request sent by the guest database program includes software licensing information, for example, a licensing identification number (e.g., an assigned installation code). Before the host database program allows access to data stored in its local database, the host database program determines whether the request for connection has been made by a licensed copy of the guest database program. In other words, the host database program determines whether the request for connection comes from a database program that is using the same software licensing information as another database program.

In one embodiment, the host database program maintains a list of all the guest database programs connected to it. Each guest database program can be identified by its software licensing identifier. The software licensing identifier can be automatically sent, for example, by the guest database program when it wants to establish a connection to the host database program. As will be appreciated, the guest database program can send the software licensing identifier along with the session information which is typically sent by database programs over the computer network in order to establish a connection. This

approach is more efficient since the session information needs to be sent to establish a connection (or session) between the two database programs over a computer network.

When the host database program receives the request for connection, it can extract the software licensing identifier. The software licensing identifier can be compared with the list of identifiers that the host program maintains. This ensures that the guest database program is not an unlicensed software copy. In this way, only one licensed copy of the database program can have access to other database programs over the computer network. Thus, Network Copy Protection can be provided for database programs.

Moreover, in contrast to conventional techniques, Network Copy Protection can be provided across various platforms and/or connection protocols. This means that unlicensed use is detected, even if another software copy of the database 202 or database 208 is operating on a different platform or using a different connection protocol than the one used by the database 202 or database 208. To illustrate, Fig. 2B depicts a computer network 250 in accordance with another embodiment of the invention. The computer network 250 includes database programs 252 and 254. The database program 252 operates in the Windows environment and can provide access to data stored in the database 204. In addition, the database program 252 may use the connection protocol IPX or TCP to communicate over the computer network 250. On the other hand, the database program 254 is operating in the Macintosh environment and can use the AppleTalk connection protocol to communicate over the computer network 250, but similar to the database program 252, the database program 254 can also use the TCP connection protocol.

The database program 252 can provide access to the remote database 206 via a connection to the database program 254 over the computer network 250. Accordingly, the database program 252 has established a connection to the database program 254 to access the database. In this situation, the database program 252 is acting as the guest to the database program 254 which is acting

as the host. As will be appreciated, while the guest database program 252 has established a connection to the host database program 254, another software copy of the database program 252 will not be granted a connection to the database program 254 and thereby access to the data stored in the database 206 will not be granted. By way of example, a database program 260, which is a software copy of the database program 252, will not be granted permission to establish a connection to the database 254 while the guest database program 252 is connected to the host database program 254.

Moreover, access will be denied by the database program 254 regardless of whether the database program 260 is operating in the Windows or Macintosh Environment. Furthermore, access will be denied regardless of whether the database program 260 uses IPX, AppleTalk, or TCP connection protocol to establish a connection to the host database program 254. Thus, Network Copy Protection can be provided for databases operating across various platforms and/or connection protocols.

To further elaborate, Fig. 3 illustrates a method 300 for providing Network Copy Protection in accordance with one embodiment of the invention. The method 300 can be implemented, for example, by the database program 254 of Fig. 2B. Initially, at operation 302, a request for connection is received by the database program. This request is typically sent by another database program (i.e., a guest database program). Next, at operation 304, a determination is made as to whether the request for connection should be granted. If it is determined at operation 304 that the request for connection should not be granted, the method 300 proceeds to operation 306 where the database program denies the request to establish the connection. The method 300 ends following the operation 306.

On the other hand, if it is determined at operation 304 that the request for connection should be granted, the method 300 proceeds to operation 308 where the database program registers the software licensing information associated with the request for connection. Thereafter, at operation 310, the database program

grants the request for connection. The method 300 ends following the operation 310.

Fig. 4 illustrates in greater detail a method 400 for providing Network Copy Protection in accordance with another embodiment of the invention. Initially, at operation 402, the guest database program sends its installation code along with session information to the host database. Next, at operation 404, the session information is received. At operation 406, the host database program extracts the guest database program's installation code from the session information. Thereafter, at operation 408, the guest database program looks up the guest database program's installation code in a list of existing connections. The list of existing connections includes the installation codes for the database programs that have established a connection to the host database program. Accordingly, at operation 410, a determination is made as to whether the guest database program's installation code has been found in the list of existing connections. If it is determined at operation 410 that the guest database program's installation code has been found in the list of existing connections, the method 400 proceeds to operation 412 where an error message is generated. This error message can, for example, be displayed by the guest database program to alert the user that, because of a licensing violation, the request for connection to the host database has been denied and access to data will not be allowed. The method 400 ends following the generation of the error message at operation 412.

On the other hand, if it is determined at operation 410 that the guest database program's installation code has not been found in the list of existing connections, the method 400 proceeds to operation 414 where a determination is made as to whether the host database program also has the capability to act as a guest database program. If it is determined at operation 414 that the host database program also has the capability to act as a guest database program, the method 400 proceeds to operation 416 where it is determined whether the guest database program's installation code is the same as the installation code assigned to the host database program. If it is determined at operation 416 that the guest database program's installation code is the same as the installation code assigned

to the host database program, the method 400 proceeds to operation 412 where an error message can be generated. The method 400 ends following operation 412.

However, if it is determined at operation 416 that the guest database program's installation code is not the same as the installation code assigned to the host database program, the method 400 proceeds to operation 418. The method 400 also proceeds to operation 418 if it is determined at operation 414 that the host database program does not have the capability to act as a guest database program (e.g., the host database program is a server database program). In any case, at operation 418, the guest's installation code is added to the list of the existing connections. Thereafter, at operation 420 a connection between the host and guest database programs is established. The method 400 ends following operation 420.

As noted above, the guest database program can send its installation code along with session information to the host database program. Fig. 5 is a block diagram representation of a session information 500 in accordance with one embodiment of the invention. The session information 500 can automatically be sent by the guest database program to the host database program. Similar to conventional session information typically transmitted, the session information 500 includes a network address field 502, a user name field 504, and a version information field 506. However, in contrast to the session information conventionally transmitted, the session information 500 includes an installation code field 508 suitable for representing an installation code associated with a software license. The installation code can be represented in the installation code field 508, for example, as string using a predetermined amount of bytes (e.g., 32 bytes, 64 bytes, etc.).

As will be appreciated, the installation code field 508 can be provided as an attachment to the end of the conventional session information fields (e.g., fields 502, 504 and 506). This approach allows communication with conventional host database programs since the installation code field can effectively be ignored by the conventional database programs. Furthermore,

sending the installation code along with the session information does not introduce much overhead since usually the session information needs to be sent to establish a connection. It should also be noted that this approach does not require establishment of a connection (or session) just so that software licensing information can be verified. Thus, including the installation code field as an attachment to the end of the session information conventionally sent by the guest database program is an efficient way of implementing Network Copy Protection for databases. In addition, this approach also provides backward compatibility with conventional database programs.

The invention can use a combination of hardware and software components. The software can be embodied as computer readable code on a computer readable medium. The computer readable medium can be any data storage device that can store data which can thereafter be read by a computer system. Examples of computer readable medium include read-only memory, random-access memory, CD-ROMs, magnetic tape, and optical data storage devices. The computer readable media can also be distributed over a network-coupled computer system so that the code is stored and executed in a distributed fashion.

The advantages of the invention are numerous. Different embodiments or implementations may yield one or more of the following advantages. One advantage of the invention is that Network Copy Protection can be implemented for database programs operating on various software platforms. Another advantage of the invention is that copy protection can be effectively provided even if different connection protocols are used by the database programs. Still another advantage is that the invention can be implemented to operate in an efficient manner and without significant change to the existing connection protocols and/or database programs. Yet another advantage of the invention is that Network Copy Protection can be implemented for more prevalent connection protocols.

The many features and advantages of the present invention are apparent from the written description, and thus, it is intended by the appended claims to cover all such features and advantages of the invention. Further, since numerous

modifications and changes will readily occur to those skilled in the art, it is not desired to limit the invention to the exact construction and operation as illustrated and described. Hence, all suitable modifications and equivalents may be resorted to as falling within the scope of the invention.

5

What is claimed is: